@DeldigiKNOW

May 2017 Issue

DEPARTMENT OF TECHNOLOGY & INFORMATION

DELIVERING TECHNOLOGY THAT INNOVATES

# eSecurity News — Be Aware of Ransomware

## Be Aware

**Ransomware** is malicious software used by cybercriminals to deny access to data or systems. The criminal holds the data/system hostage until a ransom is paid. Data can be deleted or systems locked down so owners cannot use their device or retrieve information. Even if the ransom is paid, there is no guarantee that access will be returned to the victim.

In a ransomware attack, the victim — upon seeing an email addressed to them — will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax. The attachment actually contains the malicious ransomware code. Or, the email may contain a legitimate-looking URL, but when the user clicks on it, they are directed to a website that infects their computer with malicious software.

Ransomware first appeared in 2005 and is the most widely spread threat to organizations.

## News & Resources

- Incidents of Ransomware on the Rise
- Ransomware Facts and Tips
- Ransomware Picks Off Broader Targets
- Ransomware in Government

***Questions, comments or topic suggestions?***
***Email us at*** eSecurity@state.de.us

## Be Smart

- Backup your home computers routinely.
- Don't open suspicious email links or attached files.
- Don't use links — go directly to the website from your browser.
- Keep all of your devices (smartphones, tablets, Macs, PCs) automatically patched with security updates.
- Report ransomware and phishy emails to your IT team and Information Security Officer.
- Scan USBs and other external devices.
- Use strong passwords and don't reuse them.
- Use two-factor authentication for your devices and accounts.

*For additional information visit:*
Delaware DigiKnow on Cyber Security Scams

**Breaking News!**
Hacker holds Netflix ransom...

**Visit the DTI eSecurity website for previous issues of**
**eSecurity Newsletters**

DigiKnow
CYBER SECURITY DEPENDS ON YOU

This newsletter is published by the Delaware Department of Technology and Information and sent to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or would like a printable copy (PDF), go to http://extranet.dti.state.de.us/information/dtie_information_eSecurity.shtml (links will only work if you are located in a state building or are using VPN to connect to the state network).